

AFFIDAVIT

I, Joseph A. Yuhasz, a Special Agent (SA) with the Federal Bureau of Investigation (FBI), Norfolk Division, being duly sworn, depose and state as follows:

Introduction

1. I have been a Special Agent (SA) with the FBI for the past four and a half years and I am currently assigned to investigate matters of computer intrusion and computer fraud. I have more than five years experience in using computers and various computer networks, including Windows NT.

2. The statements in this affidavit are based upon my experience and background as an SA of the FBI, upon my investigation and the investigation of other FBI agents, and my review of the pertinent evidence collected to date. Since this affidavit is being submitted for the limited purpose of securing a complaint, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts necessary to establish probable cause to believe that HELEN CARR did knowingly and unlawfully combine and conspire with one or more persons to possess, with intent to defraud and in a manner affecting interstate commerce, fifteen or more unauthorized access devices, and engaged in conduct in furtherance of the same, in violation of Title 18, United States Code, Sections 1029(b)(2), 1029(a)(3), and 2; that is, the defendant conspired to possess more than fifteen credit card account numbers that had been stolen and obtained with intent to defraud.

The February 11, 2001 E-Mail

3. AOL, located at 22000 AOL Way, Dulles, Virginia, is an Internet Service Provider (ISP) which offers its customers Internet access, e-mail, as well as other Internet services. AOL security personnel have advised me that any e-mail being sent to an AOL subscriber would be processed through AOL computer servers located in Northern Virginia.

4. On February 11, 2001, I received an e-mail message in Virginia Beach, VA, from precious44257166@aol.com, which e-mail was also sent to nineteen AOL customers in various states including Virginia, New York, Alabama, Tennessee, Texas, Illinois, Indiana, Missouri, and Georgia. The writer of the e-mail message stated that he was Steve Baldger from AOL security. The writer stated that AOL's last attempt to charge the recipient's credit card failed and suggested that the recipient should click on an enclosed link, which is text that sends someone to an Internet location, to enter new and alternate credit card information.

5. I observed that the link would take the recipient to an Internet location at www.geocities.com/asdfdsfsad/aobillz.htm. The Internet location, www.geocities.com, belongs to Yahoo!, Inc. (Yahoo), and is a location where an individual on the Internet may upload a personal Internet web page. This is not an AOL Internet location and therefore a legitimate AOL billing center would not be found at this location. After clicking upon the link, I was transferred to the Geocities web site noted above and was greeted with a window which welcomed me to AOL's

purported billing center. The window warned that providing new credit card information was mandatory in order to avoid account cancellation. The window also requested that I gather my last billing statement, current credit cards, and any relevant information. I was then directed to click upon an "OK" button.

6. After clicking "OK," I then saw what appeared to be a form from the AOL billing center. This form requested my current credit card information to include name, address, country, state, city, zip code, daytime phone number, evening phone number, credit card type, credit card number, expiration date, three digit security pin number, and credit card limit. The form also advised me to enter new credit card information to include credit card type, credit card number, expiration date, name from card statements, three digit security pin number, screen name, and password.

7. After entering information not containing my correct credit card information, I then clicked upon a button labeled, "Submit (click here!)," and then was thanked for using the AOL billing center.

8. As a result of my training and experience, I know that the web page such as the one described above has both an external appearance and an internal set of instructions. These internal instructions may be viewed on most pages by right clicking while the browser is on that page, and then clicking on the option, "view source." These internal instructions are in a language known as Hypertext Markup Language or HTML. Knowing this, I downloaded the code or program comprising the web page and forwarded it for analysis to FBI Supervisory Special Agent Mark Mikulski at the National Infrastructure Protection Center (NIPC) Special Technologies and Applications Unit (STAU).

9. SA Mikulski determined that the web page would submit the victim's information in a form to a script or program called FormMail.pl located on the Internet at www.globalserve.net/cgi-bin/FormMail.pl. SA Mikulski further advised that each question on the purported AOL form can be characterized as a field and each victim reply as a value. SA Mikulski advised that the victim's information would be submitted in a field with its corresponding value to www.globalserve.net/cgi-bin/FormMail.pl. In addition, the form automatically sets values for hidden fields or fields not seen by the victim and which cannot be changed by the victim. One such field was named "recipient" with the value kwisti_snow@yahoo.com. SA Mikulski advised that this suggested that any credit card and other information submitted by a victim using the form was likely being forwarded to this e-mail address; which was later confirmed as described below.

10. I found a description of a program by the name of FormMail.pl on the Internet at various web pages to include www.pair.com, www.3dresearch.com, and www.resource.hostway.com. These web pages describe the program as a generic form which accepts data from a form much like the one found at www.geocities.com/asdfdsfsad/aobillz.htm and sends the information to a specified user. The FormMail.pl program has one required field or

question which is the "recipient" field. The value or reply would be the location to which the information would be mailed. This field or question would most likely be hidden as in the case of the fake web page.

11. Yahoo is an Internet company which provides various Internet services including free e-mail accounts. Yahoo also owns Geocities at www.geocities.com, which gives the public a place and the tools needed to build a web page.

12. A Yahoo representative reported that the owner of the web page at www.geocities.com/asdfdsfsad/aobillz.htm had a login name of "asdfdsfsad." The Internet Protocol (IP) address which was recorded from the owner at the time of login, February 10, 2001 at 11:15 P.M. Pacific Time, was 209.166.135.40. An IP address is a four part number, much like a telephone number which every user of the Internet must have in order to connect to the Internet. Only one user can use a given IP address at any one point in time. Therefore, under most circumstances, knowledge of the combination of a particular IP address and the precise time of its use enables identification of both the ISP (the company providing connectivity to the Internet, often through a telephone line) and the ISP's account holder making use of the IP address at the time in question.

13. I then traced the IP address, 209.166.135.40, to an ISP named Stargate in Pittsburgh, PA. A Stargate representative advised that, on February 10, 2001 at 11:15 P.M. Pacific Time, IP address 209.166.135.40 was assigned to an account belonging to Judy McDonald, 712 Arlington Avenue, Jeannette, PA 15644. This representative also stated that the phone number used to dial up and to connect to that IP address was (724) 522-1416. A representative from Verizon stated that the telephone number (724) 522-1416 belongs to James D. McDonald Jr., also at 712 Arlington Avenue, Jeannette, PA 15644.

14. Information supplied by Yahoo provided additional links to the address at 712 Arlington Avenue, Jeannette, PA, and other addresses. Yahoo provided free e-mail service to the owner of the e-mail address kwisti_snow@yahoo.com. A Yahoo representative advised that Yahoo recorded the IP address of the user when this e-mail account was established and at the time when any password changes were requested on this account. This e-mail account was established on January 30, 2001 at 12:16 A.M. Pacific Time from IP address 63.178.212.238. During my investigation, I determined that an Internet user connected to this Sprint IP address using telephone number (616) 887-2313. The service address for this telephone number at that time was 116 Washington Street, Sparta, Michigan 49345, which address is discussed further below.

15. Yahoo officials also provided me with information about eight password change requests made on the e-mail account noted above. I traced two of these requests to IP addresses assigned to the ISP, Stargate. On May 14, 2001, a Stargate representative stated that only one of the IP addresses was traceable. This representative advised that the IP address (216.151.64.52) used to make a password change on March 11, 2001 to the [kwisti_snow](mailto:kwisti_snow@yahoo.com) Yahoo e-mail account

was assigned to an account owned by Judy McDonald, 712 Arlington Avenue, Jeannette, PA 15644. The telephone number used to dial up and to connect to that IP address again was (724) 522-1416.

Search of 712 Arlington Avenue, Jeannette, PA

16. On March 21, 2002, pursuant to a warrant issued by the United States District Court for the Western District of Pennsylvania, FBI agents searched the premises at 712 Arlington Avenue, Jeannette, PA. During the course of these searches, agents seized various items of potential evidence, including a laptop computer owned by George Patterson, and interviewed persons on the premises.

17. On March 21, 2002, Special Agent William Alcorn and I interviewed George Patterson. During the interview, Patterson stated that he earns money by sending unwanted e-mail messages or "spam" to Internet users and gets paid based upon the number of recipients who respond to the spam e-mail. When shown a copy of the fake AOL web page named AOBILLZ.HTM that I had printed out on February 11, 2001, Patterson stated that he recognized it as a web page which had been in his possession approximately one year before the interview. Patterson advised that he had been given the fake AOL web page by another individual, with a first name of "Kristi" or "Kwisti" in Akron, Ohio, who asked Patterson to upload the file containing the web page to the Internet. Patterson further stated that he knew that the file and web page were designed to obtain credit cards from unsuspecting people on the Internet. Patterson stated that, after receiving the web page file from "Kristi," he uploaded the web page using a free web space provider such as Geocities.

18. Patterson stated that he accumulated victims' e-mail addresses or screen names by going online and collecting them in chat rooms. Patterson stated that he and others involved in the scheme would then use a stolen e-mail account to send an e-mail message purporting to be from AOL security to the victims' e-mail addresses he collected, instructing them to click upon a link that would direct the victim to the fake AOL web page. Patterson stated that he recognized the name, Steve Balder, as being a name used in sending the fraudulent e-mails. Patterson stated that he sent the e-mail message to thousands of potential victims at one time. Each time he sent the e-mail message, Patterson indicated that he would receive between twenty to fifty victims' credit card information. Patterson stated that he collected a few hundred credit card numbers by using the fake AOL web page scheme and admitted accessing the e-mail account kwisti_snow@yahoo.com to obtain victims' credit card information. Patterson also later admitted that he also compiled credit card numbers from this same e-mail account and provided them to "Kristi."

Search of 116 Washington Street, Sparta, Michigan 49345

19. As noted above the IP address captured at the time the kwisti_snow@yahoo.com e-mail account was established on January 30, 2001 at 12:16 A.M. Pacific Time was

63.178.212.238. This IP address belongs to Sprint. A Sprint representative advised that, at the date and time noted, this IP address was assigned to an Earthlink customer with the logon "gethighk," and that this customer connected to the Internet at that time from telephone number (616) 887-2313. Ameritech advised that telephone number (616) 887-2313 was subscribed to by Kenneth R. Hyde, 116 Washington Street, Sparta, Michigan 49345.

20. On March 21, 2002, pursuant to a warrant issued by the United States District Court for the Western District of Michigan (Southern Division), FBI agents searched the premises at 116 Washington Street, Sparta, MI. During the course of this search, agents seized various items of potential evidence and interviewed persons on the premises.

21. One of the occupants interviewed was a Kenneth Hyde, Jr. During this interview, Hyde also admitted to being involved in the fake AOL billing center web page scheme. Hyde identified several other persons involved in the scheme, including a "Kristi," who Hyde advised seemed to be in control and who lived in Akron, Ohio with her mother. Hyde advised that he set up the kwisti_snow@yahoo.com e-mail account at Yahoo at the request of "Kristi" and that he, "Kristi," and another had access to this account and changed passwords. Hyde advised that he used stolen Earthlink accounts supplied by "Kristi" to access the Internet. Hyde also admitted to obtaining hundreds of account names and passwords and credit card account numbers, due to his participation in the scheme.

Search of 986 Harrison Avenue, Akron, Ohio 44314

22. On July 3, 2002, pursuant to a warrant issued by the United States District Court for the Northern District of Ohio, FBI agents searched the premises at 986 Harrison Avenue, Akron, Ohio, which was determined to be the residence of HELEN CARR and her mother. Before seeking authority to conduct this search, I learned the following facts, among others. First, a telephone number ((330) 753-5969) supplied by George Patterson for "Kristi," was identified by SBC Ameritech as being registered to HELEN CARR at 986 Harrison Avenue, Akron, Ohio 44314. Second, as a result of other information supplied by Patterson, I learned from the U.S. Postal Service that Post Office Box 698 in Lakemore, Ohio 44314, was registered to HELEN CARR and Kristi Carr. Third, I confirmed information supplied by George Patterson that "Kristi's" ISP was Road Runner. On April 22, 2002, a representative of Time Warner Cable, which provides Internet services via Road Runner, stated that HELEN CARR of 986 Harrison Avenue, Akron, OH 44314-2771, home telephone number (330) 753-5969, had an account with Road Runner. Road Runner advised that the user names for this account were HCARR and kcarr and that the account was installed on April 15, 1999 and remained active as of April 22, 2002.

23. On July 3, 2002, I participated in the search of 986 Harrison Avenue, during which various items of evidence were seized, and interviewed persons on the premises. SA Michelle A. Curtis and I interviewed HELEN CARR. CARR identified herself as being self-employed and stated that she supported herself by "spamming" (sending large volumes of unsolicited e-mail) adult pornography over the Internet using her Road Runner accounts. CARR admitted that she

was the only who accessed the computers located in the basement of the residence she shared with her then eighty-year old mother. CARR admitted to being an on-line acquaintance of a George Patterson, who she identified as living in Greensburg, Pennsylvania. CARR claimed that Patterson introduced her to "spamming." CARR admitted that she told Patterson that she was in her 20s and that, as part of this deception, she sent him a photograph of her niece and identified it as being a photograph of herself. CARR, who was then 54 years old, stated that she impersonated a younger woman in order to obtain Patterson's help in sending spam. CARR also admitted to using a screen name of "Kristi Carr" while on-line and admitted also using that name on the post office box noted above. After initially denying involvement in fake AOL billing page scam, CARR then admitted that she "spammed" a fake message from AOL seeking credit card verification for "BALA" and for Kenneth Hyde. CARR further admitted that she knew the purpose of doing so was to obtain AOL users' credit card numbers, which were to be sent to various e-mail accounts. CARR admitted that Hyde had created the kwisti_snow@yahoo.com e-mail account for her and for use in receiving credit card numbers obtained as a result of the scam. CARR stated that Kenneth Hyde lived in Michigan and that she introduced Hyde to George Patterson.

24. CARR identified two computers seized during the search as ones that she owned. During a review of the contents of these computers, several files were found on the hard drives which relate to the AOL billing page scam. These files include: (a) a web page, with the file name aolbillz2.htm, which was similar to one found on a computer owned by George Patterson and which was identified by Patterson as a file used in the scam; (b) web pages, with the file names, index.htm and index2.html, containing other versions of the fake AOL billing page like that identified by Patterson and like that I saw on February 11, 2001 when I received the fake e-mail from AOL; (c) a file named kccurl.txt, which contained a message similar to the one I received on February 11, 2001, indicating that AOL's last attempt to bill my credit card had failed and directing me to click on the link enclosed in the e-mail message to enter updated information; and (d) a file named 9_kccurl.txt, containing a message similar to that set forth in kccurl.txt.

25. Based upon the foregoing, I submit that probable cause exists to charge that HELEN CARR did, in the Eastern District of Virginia, and elsewhere, knowingly and unlawfully combine and conspire with one or more persons to possess, with intent to defraud and in a manner affecting interstate commerce, fifteen or more unauthorized access devices, and engaged in conduct in furtherance of the same, in violation of Title 18, United States Code, Sections 1029(b)(2), 1029(a)(3), and 2. I further request that a warrant be issued for her arrest and that, for the safety of personnel executing such warrant, that this complaint, the accompanying

affidavit, and the warrant be sealed, until such time as the warrant is served and HELEN CARR makes her initial appearance before a court.

Joseph A. Yuhasz
Special Agent, FBI

Sworn and subscribed before me this _____ day of July 2003 at Norfolk,
Virginia.

UNITED STATES MAGISTRATE JUDGE

SEEN AND APPROVED:

Paul J. McNulty
United States Attorney

Robert J. Krask
Assistant United States Attorney